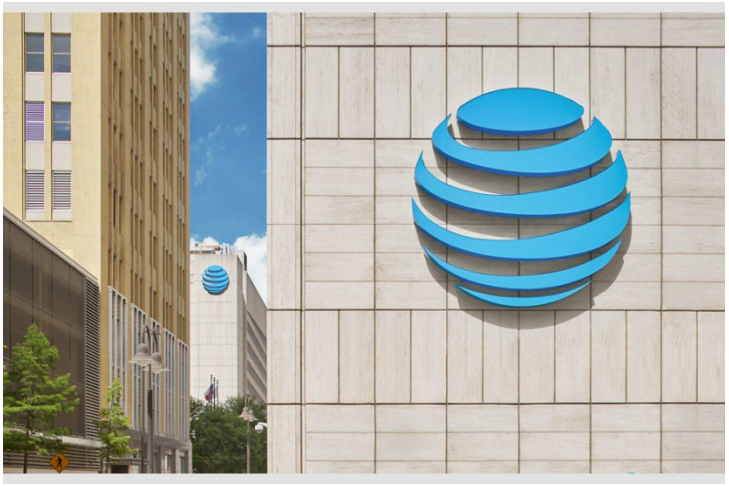

AT&T Information & Network Security

Customer Reference Guide

March 2023

Version 7.4

Table of Contents

1. To the Reader

This document is designed for the use of AT&T ("AT&T" or "Company"). current and potential business customers ("Business Customers" or "Customer"). The document provides:

- An introduction to AT&T and its global security organization
- A review of AT&T security roles and responsibilities
- A summary of Customers' security responsibilities
- An overview of AT&T security policy and comprehensive programs that strive to incorporate security into every facet of AT&T computing and networking environments. This overview focuses on the key elements and initiatives to safeguard AT&T Customers and their data while managed by AT&T or in transit on an AT&T network.

In general, the use of 'security' throughout this document refers to 'information and network security'.

For further information regarding AT&T, visit our website at http://www.att.com or contact your local AT&T account team.

2. Disclaimer

This document provides an overview of the AT&T security policy and program. To maximize security, AT&T does not divulge details regarding the tools and processes utilized to manage security. AT&T operates a common infrastructure used for its internal communications, as well as shared by its Customers. Consequently, AT&T implements and maintains commercially reasonable technical and organizational controls and measures to safeguard all data and Customers on the shared network platforms, including Customers with uniquely hosted environments and custom safeguards.

This document is provided as summary information only. It is not a contract, and no statement, representation, or characterization within this document shall be construed as an implied or express commitment, obligation, or warranty on the part of AT&T Inc. or any of its affiliates, or any other person.

All contractual obligations between AT&T and its Customer are set out exclusively in a written agreement with the Customer, and nothing in this document shall amend, modify, supplement or otherwise change the provisions or terms of that agreement.

AT&T may, in its sole discretion, alter the policies and procedures described in this document without notice to or consultation with any Customer or another person. AT&T Customers are responsible for maintaining security policies and programs appropriate to their enterprises.

3. About AT&T

AT&T Inc. is a global leader in telecommunications and technology. We help more than 100 million U.S. families, friends and neighbors, plus nearly 2.5 million businesses, connect to greater possibility. From the first phone call 140+ years ago to our 5G wireless and multi-gig internet offerings today, we @ATT innovate to improve lives.

AT&T operates one of the world's most advanced and powerful global networks, carrying more than 594 petabytes of data traffic on an average day with up to 99.999 percent reliability.

4. The AT&T Global Network

AT&T provides MPLS-based services to businesses in over 200 countries using both its own network assets as well as cross-border Ethernet, Network to Network Interfaces (NNIs), long private lines and dedicated satellite arrangements. Many AT&T customers are multinational corporations with locations in multiple global regions. AT&T is responsible for managing this worldwide data network with a presence on six (6) continents. This document provides a high-level view of AT&T's corporate approach to security, with special focus on the security of the AT&T Global Network. The AT&T Global Network is comprised of multiple components converging into a common Multi-Protocol Label Switching (MPLS) network:

- AT&T Network Cloud – cloud infrastructure hosting virtualized network functions connected to the Global IP/MPLS network
- A global Internet Protocol/MPLS backbone network
- A circuit switched network
- Ethernet, Frame Relay and ATM private networks
- Internal business and management networks
- Intelligent optical network
- Physical layer networks, including terrestrial fiber and subsea cables

5. The AT&T Labs

AT&T Laboratories (https://www.research.att.com) is the driving force behind groundbreaking innovations that transform the way people work, live and play. With a rich heritage of innovation, our teams of researchers and engineers continue to invent technologies that enable AT&T to bring a new generation of universal networks and communications to the market.

AT&T Labs is made up of the world's best scientists and engineers, including experts in Cloud services, software defined networking (SDN), mobility and wireless data networks, IP network management, optical networking technology, high-speed / broadband Internet transport and delivery systems, information and data management, and artificial intelligence. Innovations include new technologies, applications and services that support our security portfolio which enhance and provide additional safeguards to the customer experience.

6. AT&T Chief Security Office - A Worldwide AT&T Security Organization

AT&T maintains a comprehensive global security organization comprised of over 1300 security professionals. This organization, the AT&T Chief Security Office (CSO), is dedicated to the protection of the AT&T global network and its service offerings. It supports a broad range of functions, from security policy management to Customer-facing security solutions. The AT&T Chief Security Office continually reviews and assesses the Company's security posture to keep pace with industry security developments and to satisfy regulatory and business requirements. Recommendations are made on the technology solutions and critical skills that are to be developed or acquired to maintain the required security posture.

The AT&T Chief Security Office establishes policy and requirements, as well as comprehensive programs, to incorporate security into every facet of AT&T computing and networking environments. At the executive level, the Chief Security Officer chairs the AT&T Security Advisory Council, a program where key business and functional leaders meet on a regular basis to discuss corporate security strategy, vision, and concerns. The AT&T Chief Security Office's technical personnel work in partnership with other AT&T business units to evaluate threats, determine protective measures, create response capabilities, and promote compliance with best security practices.

AT&T and its employees interact with and participate in several US and international security organizations. These organizations include:

- Computer Emergency Response Team/Coordination Center (CERT/CC)
- U.S. Department of Homeland Security's National Security Telecommunications Advisory Committee (NSTAC) and its National Coordinating Center (NCC) for Telecommunications
- U.S. Department of Homeland Security's Joint Cyber Defense Collaborative (JCDC)
- U.K. National Cyber Security Centre National Security Information Exchange (NSIE)
- Australian Cyber Security Centre (ACSC) National Information Exchange (NIE)
- Various Information Sharing and Analysis Centers (ISACs), including Information Technology-ISAC and Communications-ISAC
- US InfraGard
- Security activities within the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE)

- Cyber Information Sharing and Collaboration Program (CISCP)

AT&T also participates in:

- Communication Security, Reliability, and Interoperability Council (CSRIC)
- National Telecommunications and Information Administration (NTIA)
- Network Reliability Steering Committee (NRSC)
- Communications Sector Coordinating Council (CSCC)
- US Telecom
- GSM Association (GSMA)

AT&T is proud to be a leader and a participant in these and other organizations both to set standards and to keep pace with industry developments.

7. Security Organization Mandate

AT&T considers network and information security to be a cornerstone of the services that it delivers worldwide. Through the security policy mandates and recommendations of the AT&T Chief Security Office, AT&T is committed to protecting its Customers and its own information and resources from unauthorized access, disclosure, corruption, or disruption of service. This security policy is designed to protect AT&T and AT&T managed assets, services, and is applicable to network elements, systems, applications, data, and computing devices owned or managed by AT&T.

Execution of the policy is led by the AT&T Chief Security Office whose role is to:

- Protect AT&T owned and managed assets and resources from security breaches by monitoring potential security threats, correlating network events, executing corrective actions, and enabling compliance with legal, regulatory, and contractual security requirements.
- Own and manage the AT&T security policies and standards for the entire Company and maintain ultimate responsibility for all aspects of network and information security within the Company.
- Promote compliance to AT&T security policies and network and information security program in a globally consistent manner on all networks, systems, and applications,

and hold senior executives accountable for security compliance in their business unit or region.

- Offer best-in-class security, while offering security thought leadership in the global security arena.

8. AT&T Security Standards, ISO 27001, and ISO 9001 Certifications

The primary objective of an information security program is to protect the integrity, confidentiality, and availability of Company assets. A critical component of the program is the security policy. The AT&T Security Policy and Requirements (ASPR) serve as a guide and a reference point to conducting business in a secure environment and protecting AT&T assets. ASPR is a comprehensive set of security control standards based, in part, on leading industry standards such as ISO/IEC 27001:2013.

AT&T Executive Management has produced and implemented an approved Information Security Management System (ISMS); ASPR defines the scope and boundaries of the company's ISMS. This policy defines the scope of the organizational ISMS and defines the ISMS policy in terms of the business, its location, assets, and technology. The policy provides a general framework for setting information security objectives and establishes an overall sense of direction and principals for action regarding information security. The Company takes its lead from the ISO/IEC 27001:2013 standard in further defining ISMS policy. Management commitment to Information Security Management is strong throughout the Company. Authorization to implement and operate the company ISMS comes directly from our Chief Security Officer supported fully by all other executive and mid-level management team members. AT&T maintains two global ISO/IEC 27001 certifications. The scope of these certifications covers the AT&T Global IP infrastructure and Customer facing products and services. To maintain the certifications, AT&T must undergo annual recertification assessments, which it is committed to completing and achieving ongoing certification. In compliance with the ISO/IEC 27001: 2013 standard for information security, AT&T has prepared a Statement of Applicability.

The International Organization for Standardization (ISO) is an international standards setting body comprised of representatives from standards organizations worldwide. Its purpose is to develop common standards in several different business aspects including areas such as quality, security, environmental management and social responsibility, amongst others. These standards are continuously developed to outline best practices for the area that each cover. ISO 9000 is the family of standards which cover different aspects of quality management. ISO 9001 covers the client focused aspect of quality,

which is ensuring that the client is provided the highest level of quality regarding services and products that they receive.

AT&T has achieved ISO 9001:2015 certification, which demonstrates and reinforces our belief that Customer satisfaction and expectations are the most important factors in the work we do. We are fully committed to a high standard and quality of work that we undertake for any project we undertake.

We are exceptionally proud of our achievement in the ISO 9001:2015 certification standard. However, we're not resting on this achievement and in our continuing endeavors to improve, we're also focusing on our ISO 27001:2013 certification. This standard looks at security techniques within Information Technology systems; high compliance and data security is another key factor in our internal and external operations and projects which we find gives our Customers the satisfaction and results they have come to know and expect of us at AT&T.

Additional information about the AT&T ISO 27001 certification, Information Security Management System (ISMS), and Statement of Applicability are available from your account team upon request.

Given the dynamic environment that AT&T supports, ASPR content is continually re-evaluated and modified, as industry standards evolve and as circumstances require. In addition, operating procedures, tools, and other protective measures are regularly reviewed to ensure the highest standards of security are observed throughout the Company. AT&T security policy and control standards are proprietary to AT&T and are not generally disclosed to any organization or entity external to the AT&T corporate family. Maintaining the confidentiality of this information is a facet of our security program that protects AT&T Customers.

The Enterprise Mobility Security Standard (EMSS) provides guidance for organizations to follow as they are mobilizing their operations. EMSS helps organizations develop mobile security controls to strengthen data and information protection on smartphones, IoT devices and associated ecosystems. This document is available from your account team upon request.

9. AT&T Security Programs

9.1 Security Executive Briefing and Round Tables

Security experts from the AT&T Chief Security Office frequently host Security Executive Briefings and Roundtables for AT&T Customers, analysts, and media to discuss the latest security trends and activities. They share expertise and offer guidance on security issues observed in very large and dynamic environments – such as the AT&T network – and provide advice on best practices in dealing with ever increasing threats in today's world. The executive briefings and roundtables take place at AT&T Executive Customer Briefing Centers and at public venues in major cities.

9.2 Security Training and Certificates

AT&T encourages its employees to obtain security training and to achieve accreditations and certifications. This training is conducted both within AT&T and through corporate training organizations such as:

- The International Information Systems Security Certification Consortium, Inc. (ISC)2
- Information Systems Security Association (ISSA)
- The SANS Institute
- Vendor and product-specific training and certification, such as, Cisco, Microsoft, Checkpoint, Juniper, and others.

Our large population of security professionals maintain certifications and credentials such as:

- Certified Information System Services Professional) (CISSP)
- Certified Cloud Security Professional (CCSP)
- Certificate of Cloud Security Knowledge (CCSK)
- Certified Information Systems Auditors (CISA)
- Certified Information Security Management (CISM)
- Certified in Risk and Information Systems Controls (CRISC)
- Certified Ethical Hacker (CEH)
- Global Information Assurance Certification (GIAC)

- RSA Certified Security Professional (CSP)
- Microsoft Certified Professional (MCP)
- Cisco Qualified Professional

Public Cloud

- Microsoft Azure Certification
- Amazon AWS Certification

9.3 AT&T CSO Security Center for Innovation

The AT&T CSO Security Center for Innovation was created within the AT&T Chief Security Office to drive security innovation and create what may be impossible today and revolutionary for tomorrow. The researchers work on large scale problems in dynamic areas such as mobility and cellular/5G, cloud computing, broadband, networking, Internet of Things (IoT), blockchain, NFTs and Artificial Intelligence /Deep Learning/ Machine Learning (AI/DL/ML). The Security Research Center searches for ways to leverage the power of the network for new security solutions, architectures and mechanisms. Their results and innovations become part of new systems and services that AT&T deploys for next-generation security.

9.4 AT&T Security Operations Center

The AT&T Security Operations Center (SOC) provides comprehensive security across one of the world's largest network infrastructure by deploying a proactive defense-in-depth strategy of including additional layers of security behind the network perimeter. AT&T's Security Operations Center provide a highly specialized and coordinated approach to protecting the network and services. AT&T utilizes the same set of security tools to manage its global network that it uses for its Managed Security Services available to its Customers.

The AT&T SOC is a 24x7 centralized command and control center that includes expert staff, time-tested methodologies, and proprietary technology. The SOC can monitor and analyze traffic via the AT&T IP backbone, providing advance and near real-time notification/alerts of different types of security events and produce daily company security reports.

Using a global sensor network, the AT&T SOC supports the detection and mitigation of all security events across multiple devices and device types. The SOC provides correlation and alerting, situational awareness, incident response, as well as proactive threat vulnerability analysis. It can manage threats and clean harmful traffic that may result in a business loss.

9.5 Security Awareness and Education

The AT&T Chief Security Office is charged with managing the security awareness program across AT&T. The program comprises targeted security awareness initiatives promoted internally within AT&T, an internal security awareness website, an internal awareness newsletter, all-employee bulletins and communications, and employee security awareness at on-site events. The AT&T Chief Security Office also maintains and updates the security training curriculum. The Chief Security Office provides an annual Security Awareness Corporate Compliance course. The Compliance course trains on the major cybersecurity tenets. All corporate employees are required to take this course. The Chief Security Office tracks completions of the Compliance course in conjunction with the corporate training organization.

Subject matter experts from the various security groups and disciplines support content development for web and video-based courseware. In addition, all AT&T personnel are required to annually acknowledge their responsibilities to adhere to the AT&T Code of Business Conduct, AT&T information security policy, and AT&T information protection requirements.

10. Organization of Information Security

10.1 Security Policy

It is the policy of AT&T to protect our information, infrastructure, and services, ("AT&T's Information Resources"), in all its forms from unauthorized or improper use, theft, accidental or unauthorized modification, disclosure, transfer, or destruction. This is achieved through the analysis of security risks to create security requirements that address those risks commensurate with the AT&T Information Resources' sensitivity, value, and criticality.

This policy applies to all AT&T's Information Resources which are created, used, or maintained by or on behalf of AT&T or its customers unless superseded by a customer contract.

In protecting AT&T's Information Resources, it is AT&T's obligation to comply with all applicable laws and government regulations, including those that relate to the safeguarding of personal information and critical infrastructure.

The AT&T Chief Security Office develops, maintains, and issues specific security requirements and other reference materials in support of this policy. The security requirements and reference materials comprise the AT&T Security Policy and Requirements

(ASPR) content, which is the basis for all security controls that protect AT&T's Information Resources. ASPR is not shared externally except when approved, necessary, and under strictly controlled circumstances with proper non-disclosure agreements in place.

10.2 AT&T Security Roles and Responsibilities

AT&T Security Policy & Requirements (ASPR) applies **enterprise-wide** and establishes the minimum required safeguards to protect computing and networking assets, data and services.

All Employees, Contractors, Supervisors, Application/Software Developers, System & Database Administrators, Network Architects & Operations must comply with ASPR and such responsibilities include:

- Ensuring accountability for protecting assets under their ownership and control.
- Revoking logical and physical accesses owned by an employee based on his/her job reassignment or termination from employment.
- Validating their personal logical and physical accesses to systems and facilities on a regular basis
- Maintaining and executing security status checking processes, security profile/signature upgrades, etc., on systems under their control.
- Complying with confidentiality requirements, Customer privacy agreements, government policies where applicable and necessary, and office "clean desk" programs for securing confidential information.
- Responsible for developing skills necessary to support the security function.
- Complying with the AT&T Code of Business Conduct.

10.3 AT&T Corporate Management Engagement

AT&T management is engaged with the security program. Some of the situations where management in the service lines are engaged include:

- Security incidents as they occur

- Progress from security initiatives
- Threat intelligence gathered by trend analysis; and
- Results of internal and external audits and reviews.

In addition, the management chain of command receives consolidated reports on a regular basis outlining the results of the security programs and the key issues for their area of responsibility. These reports are delivered to the senior executives as well as their line management.

Senior executives are required to annually acknowledge their commitment to support corporate compliance which includes completion of an annual compliance verification form.

11. Risk Management

The AT&T approach to identifying and mitigating network and application vulnerabilities is formalized in the Risk Management program. When vulnerabilities are identified, they are assessed as to severity, potential impact to AT&T and its Customers, and likelihood of an occurrence. Plans are developed, implemented, and tracked to address vulnerabilities within prescribed timeframes according to the criticality rating. AT&T has a formal, documented Risk Management policy and program that includes risk identification, risk assessment, risk analysis, and risk mitigation/acceptance. An extensive program of vulnerability testing, compliance reviews and security audits provide a comprehensive view of AT&T's security risk posture.

12. Asset Management

AT&T has an information classification policy that is periodically approved by management and communicated to employees.

AT&T is committed to accounting for and protecting its assets from unauthorized access. Designated components reside in secured locations, accessible only by authorized personnel, and applicable employees are required to complete annual security and access control training designed to prevent unauthorized building and equipment access. AT&T assets are tracked according to documented processes in systems maintained according to AT&T Security Policy & Requirements (ASPR) guidelines.

AT&T has numerous internal accounting control guidelines in place to manage the entire lifecycle of its assets:

- Transactions are carried out in an authorized manner.
- Transactions are reported and recorded in a way that permits correct preparation of financial statements and accurate records of assets.
- Access to assets is in accordance with management authorization.
- Comparisons between existing assets and records are made periodically, as appropriate, with action taken to correct discrepancies.

13. Human Resource Security

13.1 Background Checks

AT&T is committed to maintaining a workplace free of violence and to the protection of its employees, Customers, and assets. To promote consistency, the Company conducts background checks on the finalists for all U.S. and international employment positions. It is AT&T's practice to conduct background checks that include foreign countries to the best of our ability and within our influence. We respect the laws and customs of all foreign countries that prohibit us from conducting a complete background check. In addition to conducting background checks on all new hires and rehires, AT&T also conducts background checks on existing employees as needed, e.g., employees moving into sensitive positions, in support of Customer contracts and/or as required by law.

13.2 Personnel Security

The AT&T Human Resources organization has controls in place so that AT&T employees are properly screened and are aware of their responsibilities regarding AT&T and Customer assets in accordance with ASPR and AT&T's Code of Business Conduct.

The AT&T Supply Chain organization facilitates insertion of asset protection background check requirements into AT&T agreements with its suppliers. These requirements help to ensure that the personnel of suppliers granted physical access to AT&T and Customer premises are properly screened and are aware of their responsibilities regarding AT&T and Customer assets.

14 Physical and Environmental Security

14.1 Physical Access Control

Physical access controls are based on the principle of "Least Privilege," which strives to restrict or limit all access to only areas necessary to perform authorized functions. AT&T operates in secured environments where physical access to staff office space, switching centers, global network and service management centers and other network facilities is controlled through an enterprise-wide physical security standard that applies to AT&T companies, affiliates and contractors. Physical access to AT&T facilities is controlled with the use of an AT&T-issued Photo ID Card and one or more devices including an access card, code, biometric reader and/or Company-issued key. All access devices are approved and validated by an authorizing manager.

Critical facilities are controlled through alarming and monitoring based on physical security standard criteria and periodic audits are performed to confirm adherence to the requirements of this standard.

14.2 Environmental Security & Compliance

AT&T operates in an N+1 (Need plus one) methodology to provide the highest level of assurance for the environments such as, generators, UPS, switch-gear, HVAC, fire detection and suppression along with multiple power and networks feeds to critical facilities. Environmental Health & Safety (EH&S) assessments and reviews are conducted by AT&T Real Estate Operations (REO) at any given AT&T facility to assess compliance with applicable laws, regulations and company requirements. The internal reviews assess compliance related to underground/aboveground fuel storage tanks, hazardous materials and waste management, air emissions, water quality, and facility issues as well as key health and safety initiatives.

15 Vendor and Supplier Management

AT&T Supplier Information Security Requirements (SISR) is a minimum set of security requirements which are required in contracts with Suppliers when they are performing services for AT&T where any of the following occur:

- The collection, processing storage, handling, backup, disposal, and/or access to information when performing any action, activity or work
- Providing or supporting AT&T branded applications and/or services using non-AT&T Information Resources

- Connectivity to AT&T's Nonpublic Information Resources
- The development or customization of any software for AT&T; or
- Website hosting and/or development for AT&T.

16 Access Controls

Access controls are applied at three resource levels within AT&T:

- Operating Systems
- Database
- Application

An access request workflow system enables employee and contractor access to each of these levels. Each request requires the approval of a supervisor in the chain of command and the resource owner, which results in provisioning of access to the requested resource. Automated periodic access reviews, operational administration, compliance reporting and auditing functions are also available as part of the access controls framework.

Similar access controls are enabled in the form of Identity and Access Management (IAM) platforms for consumer, business, and FirstNet, as well as enterprise. Each of these systems has an access management and an identity lifecycle management component of functions. Access Management can be thought of as a runtime environment in which user authentication and authorization are enforced for access to protected resources, such as AT&T's wireless services. Identity lifecycle management provides identity assurance, registration, identity profile management, authenticator management for ensuring a user's identity can be validated. Followed by authorization management for assigning a user with permissions to perform functions on the resources to which they have access. Individual accountability, auditability, and forensics are enabled on these systems by logging the transactions performed by each user, each administrator, or anyone else who uses these systems for accessing AT&T resources.

AT&T uses various technologies built into our IAM platforms to assure the security and authorized access to AT&T's resources, such as the following:

- Authentication: up to 3 factors of authentication
- Federated Identity Management: typically, Security Assertion Markup Language (SAML) or OpenID Connect, either as an Identity Provider or as a Service Provider
- Authorization
- Role Based Access Control
- Attribute Based Access Control
- OAuth 2 (delegated authorization)

- Mobility device-based single sign-on access to web-based or native applications

16.1. Logical Access Control Measures

Logical access controls are based on the principle of "Least Privilege" that strives to restrict or limit access to computer resources to only the commands, data, and systems necessary to perform authorized functions. A user who needs access to AT&T and Customer services must have a current business need, must be allocated a unique identifier (a User ID), approval from their management (e.g., for employees and contractors), and must validate their identity. This access is controlled by:

- Authenticating a claimed identity to the satisfaction of an access permission-granting authority. This authentication entails all individual users being positively and uniquely identified before being granted access using one or more authentication factors such as:
    - Shared secrets (e.g., passwords, personal identification numbers (PINs) tokens)
    - Something you have (e.g., certificate, Time-Based One-Time Password to a mobile device)
    - Something you are (e.g., biometric fingerprint, biometric face print, biometric voice print)
- Having systems and network administrators or access providers review and verify with the user's supervisory manager that the User IDs, accounts, and associated command and data access permissions are appropriate for the person's job responsibilities. Where a valid business requirement does not exist for the continuance of such privileges, access is revoked.
- Controlling privileged access to systems and network elements through established security administration controls that restrict access to sensitive information, and network processors, as well as limiting the ability to set, modify or disable system security functions to authorized staff.
- Identifying and recording, through audit logging, each successful and unsuccessful access attempt, and blocking access when access attempts exceed threshold settings.

- Requiring that all passwords, passphrases, and two factors for user authentication (employee, contractor, business partner, etc.) conform to established rules. The rules for passwords specify: the minimum number and types of characters, uniqueness both from previous user passwords, as well as from username or dictionary words, avoidance of repeating characters, limitations on password sharing or group use, and requiring passwords to be changed at regular intervals. In addition, certain common passwords are blocked from being used.

16.2 Access Authorization Control

AT&T Personnel

Only AT&T personnel with a current business need are authorized with physical and logical access to facilities and systems.

Access (physical and logical accesses) is validated upon staff re-assignment or removed upon termination of employment. As a control measure, physical and logical accesses are revalidated regularly at defined time intervals to verify that the staff continues to have a legitimate business requirement for the access.

Customers

Customer authorization to AT&T services is controlled through the assignment of roles that assign privileges to perform functions within a service typically that a customer has purchased.

17 Network Element Access Controls

Current industry and AT&T-developed tools are utilized for managing the authentication and approval of support personnel to access the large population of AT&T network elements including routers, switches, and wireless access points in the worldwide network. Access is provided to AT&T technical support personnel only on an as-needed basis for individuals with responsibility for network element maintenance and support. Access to network elements supporting Customer services is controlled by:

- Using authenticating servers that validate and verify user access so that only personnel currently responsible for managing these networks have access.
- Logging all access to the authenticating servers and subsequent devices.

- Flagging repeated failed login attempts and blocking offending accounts.
- Changing passwords or passphrases for routers at regular intervals and complying with AT&T internal requirements for both.
- Reviewing passwords or passphrases on routers, or their management applications, whenever an employee possessing such a password or passphrase terminates employment with AT&T or is re-assigned.
- Using strong authentication when required, specifically two-factor token-based authentication for access to managed network elements.

18 Network Perimeter Protection

AT&T external network connections are protected by firewalls that screen incoming and outgoing traffic based on source and destination address, protocol, and port, in accordance with AT&T security policy. Internet connections and extranets are protected by firewalls and demilitarized zones (DMZs) that block any direct network routing between the internet and internal AT&T networks.

External Customer and third-party connections to AT&T networks are protected by access controls (such as access control lists or network-based firewalls) that screen incoming and outgoing packets to allow only authorized traffic.

19 Public-Facing Website Protection

Public-facing website platform applications requires protection at each of the layers: network, operating system, application, and database.

Protection for the Network and Operating system layers includes:

- User management systems maintaining user account access and type of access.
- Monitoring systems and user activities through event logging along with automated log analysis.
- Host scanning tools to assess vulnerabilities and configuration issues along with searching for malware.

- Network scanning of each device to determine potential vulnerabilities, where scanning is performed both from outside of the AT&T network in, and from inside of the corporate network out.

Protection for the application layer including database entails fulfilling the AT&T Security Policy and Requirements for Application Development and Sustainment including Mobile Applications. For example, strong authentication and change of passwords regularly are required on our public facing websites where authentication is used. New threats and vulnerabilities are addressed on an ongoing basis to protect the public-facing website platform applications against known attacks.

20 Vulnerability Management Process

AT&T utilizes an internal global program to acquire and distribute security advisories, coupled with review and compliance processes as a follow-up to these advisories. Security advisories predominantly consist of newly identified vulnerabilities and flaws to network software, systems and equipment which could potentially allow unauthorized users to bypass access controls and/or gain access to data.

AT&T continually reviews bulletins, alerts and advisories regarding security issues, patches, vulnerabilities, and exploits from vendors and organizations (such as US-CERT) for AT&T owned and managed network assets.

The vulnerability management program is also responsible for notifying system owners and or administrators to apply security patches to network systems in a timely manner. Each security advisory is reviewed, evaluated, assigned a severity rating, and published by the AT&T global security organization, which in turn, dictates the timeframe within which the vulnerability must be resolved.

21 Security Incident Reporting and Management

AT&T uses a consistent, disciplined global process for the identification of security incidents and threats in a timely manner to minimize the loss or compromise of information assets belonging to both AT&T and its Customers, and to facilitate incident resolution. Each employee and contractor is responsible for reporting suspected or suspicious security incidents.

The AT&T Global Technology Operation Centers (GTOCs) maintain 24 x 7 near real-time security monitoring of the AT&T network for investigation, action and response to network security events. AT&T Threat Management platform and program provides near real-time data correlation, situational awareness reporting, active incident investigation and case management, trending analysis, and predictive security alerting.

If AT&T discovers that a party has obtained unauthorized access to customer's data during a security incident on AT&T's network and/or data storage facilities, AT&T will promptly conduct an investigation to determine when, and if possible, how the incident occurred, and will promptly notify the customer consistent with all applicable laws and regulations.

Incidents are reported to the AT&T Computer Security Incident Response Team and, if appropriate, senior management to draw attention to the types of attacks reported by our incident response team as well as other noteworthy incident and vulnerability information.

22 Intrusion Detection Services/Intrusion Prevention Services (IDS/IPS)

AT&T employs a combination of internally and commercially developed tools to detect attempts by unauthorized persons to penetrate the AT&T Global Network. AT&T does not monitor individual Customer connections for intrusions, except when part of a managed security service. For Customers who have subscribed to this component of managed security service, AT&T will promptly notify the Customer if it believes that a detected intrusion attempt may impact the Customer's service.

23 Distributed Denial of Service

AT&T employs a combination of internally developed and commercial tools to detect and mitigate Distributed Denial of Service (DDoS) attempts by unauthorized persons to penetrate the AT&T Global Network. AT&T does not monitor individual Customer connections for intrusions, except when part of a managed security service. For Customers who have subscribed to this component of managed security service, AT&T will promptly notify the Customer if it believes that a detected DDoS event may impact the Customer's service.

24 Workstation Security Management

The workstation security policies protect AT&T and Customer assets through a series of processes and technologies including, but not limited to, verification of personnel workstation

accesses, endpoint (anti-virus and anti-malware) protection, Operating System hardening and updates, full disk encryption where permitted by law to protect sensitive information on portable assets, along with a firewall intrinsic to remote access software implemented on workstations or portable PCs that remotely connect to the AT&T network. AT&T also limits the administrative capabilities of each workstation.

Securing of the personal computer while in use is further managed by the requirements for log-on passwords, hard drive passwords where possible, and password-protected keyboard or screen-locks that are automatically triggered through inactivity. Management at AT&T is responsible for ensuring compliance with these policies.

AT&T workstations are required to have active endpoint protection software. AT&T's endpoint protection software vendor provides threat protection updates which are referenced automatically by workstations across the Company. Updates are provided continuously, including in the event of an outbreak, via the vendor's cloud-based solution. Furthermore, security advisories forwarded by the AT&T Chief Security Office provide information regarding security threats and mitigation strategies to AT&T personnel.

25 Change Management

To maintain the integrity of the security infrastructure, AT&T uses documented change management processes to submit, approve, and report change requests. A new change request initiates scheduling of a maintenance activity and approval processing. Change requests must receive the appropriate approvals prior to being performed.

The scope of the AT&T change management program includes, but is not limited to:

- Installing, removing, or modifying software
- Modifying configuration parameters including Operating System (OS) and application security logging and security parameters
- Upgrading to a new release level
- Installing patches or fixes
- Invasive system or process testing
- Changes to application software
- Changes to hardware (physical and virtual)

- Changes to the network or network elements (physical and virtual)

26 Security Status Checking and Vulnerability Testing

26.1 Security Status Checking

- Status Checking is performed by centralized tools on a regular basis to review and verify system security settings, computer resource security settings and status, and users having security administrative authority or system authority.
- Verification of authorized software compliance
- Status Checking includes the testing of network elements to verify the proper level of security patches, and to confirm that only required system processes are active.
- Validation of server compliance to AT&T security policy is conducted on a regular basis on AT&T servers.

26.2 Vulnerability Testing and Security Analysis

Vulnerability Testing is performed by authorized personnel to determine whether controls can be bypassed to obtain any unauthorized access.

- Vulnerability tests to evaluate the level of safeguards on network components are performed on a varying frequency based on the risk of compromise and other factors, utilizing authorized leading-edge testing tools.
- Vulnerability scans are conducted on networks, computer hosts and applications owned by AT&T at regular intervals as directed by AT&T security policies using AT&T-developed tools and leading-edge scan tools from recognized commercial software providers.

Network or computer security analysis is commonly referred to as intrusion testing, penetration testing, sweeps, profiling, and/or vulnerability analysis. Performing security analysis of the AT&T networks or computers or applications is the responsibility of AT&T. Performance of security analysis by Customers is expressly prohibited unless written approval has been obtained from AT&T.

26.3 Security Status Reporting

Information regarding the security status of the AT&T infrastructure and services is managed and communicated on a need-to-know basis. Results of security health checking and vulnerability testing are tracked and reported by the security programs responsible for compliance management of those activities. Security status, as well as progress on security initiatives, is combined with threat intelligence gathered through trend analysis and reported to security organization executives.

Security program managers share security status information to promote alignment of program objectives and prioritization of efforts. This disciplined sharing of security status information and reporting enables AT&T to achieve synergy and cooperation among security teams and appropriate management attention to the AT&T overall security posture.

27 Compliance

27.1 Security Compliance Reviews

AT&T conducts regular internal reviews of operations and applications functions for compliance with AT&T Security Policy and Requirements (ASPR). AT&T considers such reviews as essential to evaluating the adherence to the established security procedures worldwide. Results of these reviews are reported to AT&T regional security managers and executive management. Results of routine internal reviews are not typically shared with Customers, except as warranted by applicable auditing standards

Security reviews may be facilitated or conducted by the AT&T Chief Security Office; by a business area sponsor of a product, service, or supplier or partner relationship; or by an operations team responsible for life-cycle service management. Business and operations areas are encouraged to perform self-reviews to verify compliance with published security requirements.

An internal review of compliance with security requirements is a comprehensive review of an organization's adherence to regulatory guidelines and internal policies, controls, and procedures, as applicable. Security auditors or assessors evaluate the strength and thoroughness of compliance. Assessors review security policies, user access controls and risk management procedures over the course of a compliance engagement and report the findings to all key stakeholders.

27.2 Internal and External Reviews and Audits

In addition to the security compliance reviews, AT&T conducts regular internal and external reviews to assess compliance with regulatory, industry, corporate governance, and privacy requirements. For certain Services, AT&T retains external auditors for audits and certifications of AT&T's security practices and controls against various standards, such as Sarbanes-Oxley, SSAE18/ISAE3402, and Payment Card Industry (PCI) Data Security Standard (DSS), the Information Security Standard (ISO/IEC 27001), and the Quality Management Standard (ISO 9001) in the following areas within AT&T: Network Operations, Supply Chain, and Government Solutions).

AT&T has adopted the Statement on Standards for Attestations Engagements (SSAE) in conjunction with the International Standard on Assurance Engagements (ISAE). SSAE 18/ISAE 3402 standard as the professional standard for service organizations to obtain an independent assessment about the effectiveness of internal controls that are relevant to our Customer's financial statements. An examination under this standard signifies that a service organization has had its control objectives and control activities, including controls over information technology and related processes, examined by an independent accounting and auditing firm. A formal report containing the auditor's opinion, detailed control descriptions, and test results is issued to the service organization at the end of the examination. This formal report is referred to as a Service Organization Control (SOC) Report.

AT&T plays multiple roles in PCI compliance - one being a Merchant and the other being a Service Provider. AT&T serves as Merchant because it accepts credit cards as payment for goods and/or services. AT&T serves as a Service Provider as it may store, process, or transmit cardholder data on the entity's behalf or serve as a managed service provider that manages components of the entity's cardholder data environment, such as routers, firewalls, databases, physical security, and/or servers.

Additional information about external audits and certifications relevant to the Services is available from the Customer's AT&T account team upon request. AT&T will provide applicable audit reports to Customers that AT&T undertakes as part of its general business operations. Such reports are AT&T's Confidential Information and will be subject to restrictions on use and disclosure.

AT&T will engage in general security discussions with client executive representatives to address questions or concerns from their Customers or the Customer's auditors. However, security reviews conducted by AT&T Customers or their representatives are only permitted under specific terms and conditions, including non-disclosure, and require express written

authorization from AT&T concerning the scope and frequency; a fee may be charged as well to cover the cost.

27.3 Compliance with Standards and Regulations

AT&T's Code of Business Conduct is the foundation for how we do business, and how we treat each other and our Customers. The Code puts our values in action and guides us to the right decisions every day. Each employee is responsible for being familiar with the information in this Code and for following the Code and the Company's policies and guidelines.

AT&T possesses sensitive, detailed information about our Customers, who rely on AT&T to safeguard that information. Laws and regulations tell us how to treat such data. Any inappropriate use of confidential Customer information violates our Customers' trust and may also violate a law or regulation. Preserving our Customers' trust by safeguarding their private data is essential to our reputation. We are diligent about following the laws and regulations that relate to our business. The Company's internal policies and procedures support and clarify these laws and regulations and facilitate our compliance. Our business has grown into many parts of the world. While our goal is to conduct business consistently across the globe and in accordance with the principles of this Code, we adjust our practices to comply with the laws and requirements of our diverse markets.

AT&T complies with legal, regulatory data protection and privacy controls relevant to its services in the countries where we do business (e.g., GDPR, CCPA). AT&T processes and programs are designed to support external corporate compliance regulations (e.g., Sarbanes-Oxley, ISO 27001, and Payment Card Industry certifications), as well as with standards applicable to AT&T commercial activities.

Subject to availability, AT&T offers custom network services as well as managed security products and services that can support Customer compliance with certain regulations in applicable countries. Examples include the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and security standards as specified through governing bodies such as the European Union. To the extent that AT&T personnel require access to information subject to privacy regulations, such information is used only for rendering service to the Customer, network management, service assurance, or as the Customer has otherwise expressly authorized.

28 Business Continuity Management

Planning for and responding to crises is something that AT&T performs on a routine basis. The company has extensive experience responding to a wide variety of situations, both anticipated and unanticipated situations.

AT&T maintains a Business Continuity Management Program (Program) to help prevent or mitigate service disruptions and aims to respond to any loss of essential AT&T business processes or AT&T services as quickly and safely as practicable. A global team of industry-leading, certified, and experienced business continuity experts are responsible for the implementation of the risk-based approach to document, certify, and maintain business resumption plans on an annual basis or as business conditions require greater frequency.

The Program is ISO 22301 certified, initially obtained in 2015 under the U.S. Department of Homeland Security Voluntary Private Sector Preparedness Program (PS-Prep™). Maintaining this recertification demonstrates AT&T's continued commitment to resume business operations and customer service delivery in the vital hours and days after a disaster strikes. AT&T is also aligned and/or certified to the:

- Disaster Recovery Institute International Professional Practices
- CTIA, as part of its Business Continuity/Disaster Recovery Program
- National Incident Management System
- ISO 27001 pertaining to Information Security Management

29 Network Disaster Recovery

AT&T's Network Disaster Recovery (NDR) team provides recovery solutions and support for Network disaster responses in the U.S. and across AT&T's Most of World (MoW) service areas. NDR's inventory includes portable generators, emergency communications assets, telco technology recovery trailers, hazmat response trucks, and a broad array of logistical support equipment including command centers, fuel trailers, and bunk trailers.

NDR's technology, asset management, and emergency communication teams are continually evaluating emerging technologies that will improve our readiness to respond. NDR partners with other AT&T Network organizations to provide proactive disaster response solutions. NDR maintains and stages assets at more than twenty warehouses and equipment yards allowing for a rapid response across AT&T's service footprint.

NDR's core team ensures the physical and technological readiness of the recovery equipment to enable asset deployment anywhere in the U.S. and worldwide—7x24x365. NDR uses a large pool of AT&T employees from across all business units to be emergency responders during

times of need. They physically deploy, turn-up, and recover the assets as needed; that capability is built and sustained using hands-on training exercises.

30 Privacy

Customer information is accessible only to those authorized to access and view it. AT&T has implemented a six-tiered Information Classification framework for categorizing information based on sensitivity of the content and legal requirements. Document markings are specified for each data classification to identify the means and levels of protection required to safeguard information in each classification.

Customer information managed by AT&T is protected by a standard privacy policy applicable to all employees and contractors, and a Code of Business Conduct that includes consequences for an employee's violation of obligations to protect personally identifiable information. AT&T personnel receive periodic awareness and compliance training to reinforce the Company's privacy standards.

Certain Customer information managed by AT&T, as defined by applicable contract terms, or classified as Sensitive Personal Information (SPI), such as Social Security numbers, credit card numbers and mobile device location, is given significant protection, including encryption (where permitted by law) when stored on AT&T networks.

AT&T employs information and data destruction and sanitization procedures to physically destroy, shred, erase or wipe electronic and physical media used to store proprietary data and information in accordance with commercially accepted practices when the media is no longer required for business purposes or hard copy leaves the control of the company. Equipment containing storage media are checked so that any proprietary data and licensed software has been removed or securely overwritten prior to disposal.

The AT&T Chief Privacy Office maintains the AT&T privacy policy. This privacy policy is available at (https://att.com/privacy). Compliance with legal and regulatory privacy requirements is addressed in the "Internal and External Reviews and Audits" section.

31 Strategy of Continuous Advancements

The world of networked computing - especially for today's mobile, always-connected devices and applications, as well as cloud environments - is fast moving and highly dynamic. Thus, AT&T is continually advancing security through active security research and development

programs, involvement in standards organizations, tracking of industry developments, and evaluation of new security technologies and products. New tools and systems are regularly evaluated and deployed as necessary. New security architectures, taking advantage of the latest advances in virtualization, artificial intelligence, and networking, are designed and implemented to protect the mobility-and-cloud-based enterprise in the era of large scale, sophisticated attacks.

32 Customer Security Responsibilities

AT&T Customers are responsible for establishing and implementing appropriate technical and organizational policies and procedures to safeguard its data and sensitive information against unauthorized access or use, and any connection to the AT&T Global Network from loss, disclosure, unauthorized access, or service disruption. The Customer is expected to promptly notify AT&T of any actual or suspected security incidents or vulnerabilities relating to AT&T services of which the Customer becomes aware.

Customer programs should address, at a minimum, physical, and logical security, and confidentiality of data. The Customer should designate a member of its management team to be the owner of its security policy and program. The Customer's security obligations include, but are not limited to:

- Responsibility for protecting the Customer's confidential information from disclosure.
- Responsibility for the management of Customer data, content and transaction information stored on or transmitted over the AT&T Global Network, e.g., backup and restoration of data, erasing data from disk space that the Customer controls.
- Responsibility for the selection and use of appropriate services, security features, and options to meet the Customer's business and security requirements, such as encryption to protect privacy of personal information.
- Responsibility for developing and maintaining appropriate management and security procedures, such as, physical, and logical access controls and processes, (e.g., application logon security, including unique user identifications and passwords/pins/tokens complying with prudent security policies) on any Customer provisioned and managed networked devices and systems.
- For "Client Managed" Customers who retain administrative control of their environment or portions thereof, sole responsibility for their own patch management,

including the review, assessment, and application of patches. Under these circumstances, the Customer assumes all risks due to vulnerability exploitation, including any additional usage charges due to such incidents. AT&T may disconnect a "Client Managed" Customer from the network if AT&T finds them to be infected with a virus or other malicious code such that AT&T or its other Customers could be placed at risk. If they choose, "Client Managed" Customers may upgrade their service level to "AT&T Managed", in which case AT&T network and information security policies and procedures will then apply.

- Responsibility for the protection and physical security of devices and systems on the Customer's premises, including preventing unauthorized sensors, sniffers, and eavesdropping devices from being installed in the Customer's premises.
- Responsibility to ensure no security testing or scanning, etc., sourced by the Customer occurs on network or application components outside the responsibility and ownership of the Customer.
- Responsibility to ensure that its end users comply with applicable laws and with the AT&T Acceptable Use Policy (found at https://www.att.com/legal/terms.aup.html) in using any service offered by AT&T that is provided over or includes access to the Internet.
- Responsibility for the acts and omissions of the Customer's end users of any service obtained from AT&T.
- Responsibility to notify AT&T promptly of any security breaches detected by the Customer related to the services provided by AT&T.

Many country laws (for example, in the United States) prohibit unauthorized access to data transmitted over a public network or commercial carrier (e.g., Internet) and unsecured transmission lines (e.g., cellular, radio or satellite). However, these open transmission services offer increased opportunity for unauthorized parties to discreetly obtain transmitted data. Consequently, all transmitted data containing information that Customer wants to protect should be encrypted when transmitted across such networks or lines. Responsibility for encryption of data traffic is solely the responsibility of the Customer data owner.

AT&T serves customers with widely varying privacy and security requirements. These include agencies of federal, state, and local governments and, in addition, firms in the financial and health care sectors covered by industry specific laws and regulations requiring the

protection of personal and private information. AT&T complies with all legal and regulatory privacy controls relevant to network services. We recognize that our customers are not only required to protect such information but also may have duties to document the manner in which they and their providers have done so.

AT&T expects that customers' specifications will include specific line-item level requirements regarding compliance with special laws and regulations, to the extent that these laws and regulations apply to AT&T's provision of services. While some obligations are owned by AT&T, others are owned by the customer, so it is the customer's responsibility to define custom requirements to meet their needs. The specific manner in which we meet customer requirements will depend on the nature of the networks, products, and services we are asked to provide. We view these specific requirements as matters of network, product, and service design.

33 Summary

AT&T is one of the world's largest communications companies and is recognized as a leading provider of IP-based communication services to businesses and consumers. AT&T views security as a process, driven by management direction/directives, by user awareness, and supported by expert skills and advanced technology. The security policies, programs and initiatives outlined throughout this document are administered worldwide by AT&T's Chief Security Office.

This document provides an overview of AT&T security policies and programs and how they are designed to safeguard AT&T Customers and their data while managed by AT&T or in transit on an AT&T network. This document also provides a summary of the Customer's security responsibilities to protect their greatest assets and heightens their awareness of why they should implement security measures.

34 Appendix

34.1 AT&T Managed Services

- **AT&T Managed Services** take advantage of the security of the AT&T global Internet Protocol/Multi-Protocol Label Switching (IP/MPLS) network. MPLS technology enables the creation of feature-rich network-based services coupled with AT&T management expertise, tools, and automation. AT&T Network-based managed services include AT&T Virtual Private Network (AT&TVPN) Service, AT&T Dedicated Internet, and AT&T Flexware Service and AT&T SD-WAN

- **AT&T Virtual Private Network (AVPN) Service** is a network-based IP VPN solution that provides a menu of transport capabilities in over 195+ countries.. It combines the flexibility of Ethernet and IP access with an advanced MPLS core to provide reliable highly secure Multi-Site connectivity Customers can build an application-aware VPN to link global locations, enabling efficient transport of voice, data and video via a single connection. This solution supports Customer managed routers and AT&T managed firewall and intrusion detection services. **AT&T NetBond Service** provides a private virtual IP network connection between a supported cloud service provider and a supported AT&T network service using Virtual Network Connections (VNCs) provided by AT&T.

- **AT&T Dedicated Internet** helps Customers consolidate management of their Internet applications with high-speed dedicated access, optimized performance and security. This service provides proactive 24x7 network monitoring, enhanced network security features, and maintenance of the communications links between Customer locations and the AT&T network. Customers can select a completely AT&T-managed solution or can choose to self-manage components of their Internet solution.

- **AT&T FlexWare** (previously known as AT&T Network Functions on Demand) is a managed service that allows Customers to deploy and use one or more Virtual Network Functions in conjunction with associated AT&T Equipment which may be included in the Customer's solution. Virtual Network Functions are networking capabilities, such as routing, SD-WAN and firewall that have traditionally been implemented in single-purpose hardware appliances and can now run as virtualized software instances at various Sites across the Customer's network.

- **AT&T SD-WAN (Software-Defined Wide Area Network)** is a networking approach that uses a centralized control function incorporating user defined application and routing policies, to provide highly secure, dynamic, application-aware network traffic management and is available in various connectivity types to fit Customer's business needs. This solution can provide centralized management of the network giving Customers visibility into network and applications performance, allowing more control of the network as well as costs and capital expenditures.

34.2 AT&T Security Products and Services

AT&T offers managed security products and services to its Customers, designed to assess and protect their vital network infrastructure. Our cybersecurity platform is equipped with tools,

processes and people with the necessary expertise to help Customers prevent, detect, and respond to evolving threats. In addition, with AT&T Cybersecurity Consulting solutions, AT&T has the flexibility and expertise to custom design solutions to meet Customer needs. AT&T Managed Security Products and Services include:

- **AT&T Managed Threat Detection and Response (MTDR)** is a sophisticated managed detection and response (MDR) service that helps you to detect and respond to advanced threats, both on premises and in the cloud. It builds on our decades of expertise in managed security services, our award-winning Unified Security Management (USM) platform for threat detection and response, and AT&T Alien Labs threat intelligence. Managed Threat Detection and Response has a dedicated security operations center (SOC), providing 24 x 7 proactive security monitoring, alarm validation and incident investigation, and security orchestration and incident response automation.

    - **USM Anywhere™** delivers powerful threat detection, incident response, and compliance management in one unified platform. It combines the essential security capabilities needed for effective security monitoring across your cloud and on-premises environments: asset discovery, vulnerability assessment, intrusion detection, endpoint detection and response, user and entity behavior analytics (UEBA), SIEM log management, continuous threat intelligence, playbooks, automation and orchestration.

    - **USM Anywhere™ Advisors** provides for reactive support, including platform tuning, configuration, and incident investigations, for a pre-defined number of monthly hours. This is available for clients using USM Anywhere™ to manage their security environment but need a bit of help at times to optimize their deployment.

- **AT&T Threat Detection and Response for Government** is FedRAMP authorized at the Moderate Impact Level and built on our award-winning Unified Security Management (USM) platform, which combines threat detection, incident response, and compliance management. Featuring built-in integrations with other IT and security tools, our single-pane-of-glass view provides visibility across your environment, both on-premises and in the cloud. AT&T Threat Detection and Response for Government is faster to deploy and easier to use than other threat platforms, allowing your security teams to begin discovering threats sooner.

- **AT&T DDoS Defense** is a Distributed Denial of Service (DDoS) attack identification and mitigation capability within the AT&T network cloud providing increased protection from malicious traffic by eliminating it before it reaches the Customer's network.

- **AT&T Authentication Verification Services (AAVS)** is a service that provides enterprises with consented access to AT&T mobiles subscriber data to authenticate a user through the use of subscriber, device data, and network data. The service is delivered as a network-based service via Application Programming Interfaces (APIs) and allows enterprises to integrated fraud defense into new or existing applications and processes

- **AT&T Premises-Based Firewall Service** is a managed network security service that provides the first layer of defense between a local area network (LAN) and the Internet. Premises-Based Firewall Service includes all hardware and software components, configuration, installation, and day-to-day management and maintenance backed by expert customer support and proactive network monitoring. **Email and Web Security Solutions** include **AT&T Secure Network Gateway Service**, an integrated, turnkey security solution allowing Customers to bundle AT&T Network-Based Firewall Service, and AT&T Web Security Service on one convenient contract and bill. The service offers a single pricing schedule with multiple service and term discounts. **AT&T Web Security** offers URL blocking and application filtering of malware for Web traffic with real-time reporting of service results.

- **AT&T Endpoint Security Services** encompass a variety of Endpoint Protection, Endpoint Detection & Response, Unified Endpoint Management and Mobile Threat Defense solutions helping customers secure and manage endpoints running Windows, macOS, Linux, Android and iOS. These solutions use threat intelligence & research as well as advanced Machine Learning methods to identify and stop attacks including Ransomware and other malware. These solutions also notify OS vendors and users of required OS upgrades, patches or other remediation actions. The management solutions work in conjunction with the security solutions to help enforce security policies across traditional (Windows/macOS), servers (Linux) and mobile (Android/iOS) endpoints. AT&T Endpoint Security Services serve organizations of all sizes in Commercial and Public Sector market segments.

- **AT&T Government Trusted Internet** - A fully managed, CISA-compliant, and scalable cloud-delivered security service, AT&T Government Trusted Internet

adheres to the TIC 3.0 initiative while providing security protection for federal agency connections. In addition to significant security capabilities, AT&T Government Trusted Internet includes a multitude of capabilities, including the CISA standard on TIC capabilities and optional Zero Trust Network Access (ZTNA) with 24/7 Security Operations Center (SOC) and Security Operations and Analysis Center (SOAC). AT&T Government Trusted Internet uses AT&T Direct Internet (ADI) as its transport mechanism for branch offices. Features apply to traffic that has been forwarded to the service.

- Next-Gen Firewall (FWaaS)
- Data Loss Prevention (DLP)
- AT&T Secure Web Gateway
- Enhanced protection from unknown threats with cloud protection
- Intrusion Prevention System (IPS)
- Cloud Access Security Broker (CASB) functionalities
- Threat detection with advanced analysis
- IPsec VPN and SSL decryption
- Traffic logging for visibility, compliance, and correlation
- Threat correlation with OTX
- URL filtering
- Transparent DNS security
- Traditional use case – security features available under AT&T MTIPS

- **Cybersecurity Consulting Services** provide Risk Advisory Services, Cyber Operations and Cyber as a Service (CaaS). Solutions range from security strategy development, program design, technical assessments that help evaluate security posture, strategy, risk & compliance consulting, security operations consulting including vulnerability management, and security response consulting including incident response, remediation, and post mortem analysis that help align security with business objectives, assessments that help evaluate security posture and meet compliance requirements and technical security assessments from a network and application perspective to keep abreast of the threat environment.

  The increasing frequency, sophistication, and ever-changing nature of cyber intrusions and data breaches continually challenge organizations' cyber mitigation and risk management teams. Cybersecurity expertise can help organizations handle the scale and complexity of their cybersecurity needs.

Tailored to your specific business environment and requirements, AT&T Cybersecurity Consulting Services address the essential elements of cybersecurity, from strategy, governance, and enterprise risk management to controls architecture, implementation, and management.

Our solutions, powered by AT&T Alien Labs Threat Intelligence, focus on aligning business objectives and IT needs to fit your organization with Information Security and Risk Management. These services provide comprehensive analysis of your security requirements against industry standards and best practices, prioritize risks and identify controls and remediation opportunities.

AT&T Cybersecurity Consulting also provides a suite of infrastructure, security operations, transformation, threat management and vulnerability services. These services improve security operations to allow organizations to accelerate adoption of emerging technologies, prioritize resource allocation and provide better orchestration across the security fabric.

They also help resolve all aspects and impacts of cyber breaches with technical investigation, forensics, containment and recovery. An incident response team can help improve time to containment and prevent threats with experts who know the organizations and environment.

At AT&T, we help organizations minimize risks, manage security operations effectively and work toward compliance requirements are met.

AT&T Cybersecurity Consulting Services can help you:

- Connect the Business and Security Goals
- Drive Faster, More Efficient Security Response
- Know and Improve Your Security Posture

Our services address regulations such as:

- PCI
- HIPAA/HITECH
- ISO 27001/27002
- FISMA/Fed Ramp
- GLBA

AT&T Cybersecurity Consulting helps provide edge-to-edge security solutions in today's evolving threat landscape with a multi-layered approach.

- **Vulnerability Management** – AT&T Consulting will utilize best in class vulnerability tools along with a risk-based assessment to implement and manage a vulnerability program customized to your needs.
- **Risk Management** – AT&T Consulting can assist with an effective risk management program operated in close alignment with business goals to include risk and strategy.
- **Incident Response** -AT&T Consulting can conduct an investigation or supplement internal cybersecurity and legal teams.
- **Security Operations**- AT&T Consulting can transform your Security Operations Center (SOC) with next-generation security technologies including defining service goals, assess current environments, identify remediation opportunities, and develop your roadmap.
- **Compliance**- AT&T Consulting can help you adhere to regulatory compliance requirements and meet strategic business objectives in a cost-effective manner.
- **Emerging Technology**- AT&T Consulting will provide guidance with Mobility, Cloud security strategy, IoT Security, and Security innovation.

For further information on AT&T Consulting, ask your account team or visit https://www.business.att.com/solutions/Family/cybersecurity/consulting.

These products and services may not be available in all regions. For more information on these and other products and services, please visit http://www.business.att.com or contact your AT&T account team.